ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 6, June 2017

PRESERVING LOCATION PRIVACY AND ENHANCING SECURITY IN WIRELESS SENSOR NETWORKS

Ms.S.Megala and Mrs.S.Devapriya, Associate Professor

Abstract*— In wireless sensor networks (WSNs), location of event reported by a sensor network need to remain anonymous. That is unofficial observers must detect inadequate origin of such events by analyzing the network traffic known as the source anonymity problem, this problem is important in security of wireless sensor networks. However most existing method either fail to provide adequate protection, or incur high communication overheads and delay. In this proposed method can improve security of wireless sensor networks (WSNs) through maintaining privacy in source location and destination place and eavesdropper can eliminated from wireless network based on community attributes. In comparison to the resource efficient traffic normalization schemes, this method reduces the communication overhead by more than 92% and end to end delay is cut more than 60% by using appropriate routing protocol such as Enhanced Dynamic Source Routing with Source Receiver Privacy(EDSR-SRP).

Index Terms*— Eavesdropper detection, Location privacy Source anonymity and Wireless sensor networks (WSNs).

I. INTRODUCTION

Wireless sensor networks (WSNs) have shown great prospective in reorganize many applications including area monitoring, health care monitoring, environmental/earth sensing and industrial monitoring, smart buildings, cities, and smart infrastructures. Several of these applications involve the communication of sensitive information that must be protected from unauthorized parties. As an example consider the medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are fitted inside human body. There are many other applications too e.g., body position measurement and location of the person, overall monitoring of sick patients in hospitals and at homes. Body-area networks can collect data about an individual's health, fitness, and energy expenditure. Privacy in sensor networks can classified in to two types, content privacy and contextual privacy: Threats with content privacy arise due to the power of adversaries to observe and manipulate the content of packets sent over a sensor network. This type of threats is countered by encryption and authentication, though WSN still exposes contextual information about the traffic carried in the networks, which are refer to event related parameters, There are three parameters that can be associated with an event detected and reported by a sensor node: the description of the event, the time of the event, and the location of the event [1], [2].

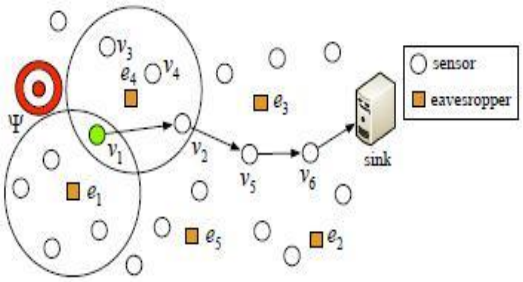

Fig.1: Detection of event Ψ by eavesdropper e_1-e_2

As an example, consider the detection of event Ψ by sensor v_1 in sink in Fig.1. Sensor v_1 forwards the event report to sink though v_2, v_5 and v_6.Transmission related to this report are intercepted by eavesdropper e_1-e_5.The event location can approximated to the sensing area of v_1.The later can be estimated as the interception of the reception areas of e_1 and e_4, which overhears v_1's transmissions. Moreover, the event occurrence time can be approximated to the overhearing time of v_1's first transmission.

.

II. PROCEDURE FOR PAPER SUBMISSION

The major contributions of this project are eavesdropper location can be detected and eliminating from wireless network by monitoring neighboring node to entire network. To provide privacy for source location to improve security in wireless sensor networks. The confidentiality of the information is protected using standard cryptographic methods.

A. Detecting Eavesdropper

Local Eavesdropper is a local adversary can intercept a limited number of transmissions within the WSN. Typically, this adversary deploys a single or a few mobile devices that

Manuscript received June, 2017.

***First Author name**, Electronic and Communication Engineering, Jayaram College of Engineering and Technology. Trichy, India,9750145058.*

***Second Author name**, Electronic and Communication Engineering, Jayaram College of Engineering and Technology, Trichy, India.*

attempt to localize source by backtracking the intercepted transmissions. A sensor with a real packet for transmission forwards it to one neighbor on the shortest path to the sink.

B. Eliminating Eavesdropper

In this analysis, eavesdroppers are limited to recording the transmission time and content hash for each intercepted packet. Limit the recorded transmission attributes to make this analysis broadly applicable to several models including WSNs that apply packet encryption (including headers), identity anonymization (e.g., via rolling pseudonyms), and other kinds of privacy protection (location, temporal, routing path).

C. Enhanced Dynamic Source Routing Protocol With Source Receiver Privacy

The *Enhanced Dynamic Source Routing* protocol (EDSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. EDSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of *Route Discovery* and *Route Maintenance*, which work together to allow nodes to discover and maintain *source routes* to arbitrary destinations in the ad hoc network.

Overview and Important Properties of the Protocol

The EDSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the sensor networks:

Route Discovery (Fig.2) is the mechanism by which a node **S** wishing to send a packet to a destination node **D** obtains a source route to **D**. Route Discovery is used only when **S** attempts to send a packet to **D** and does not already know a route to **D.** *Route Maintenance (Fig.3)* is the mechanism by which node **S** is able to detect, while using a source route to **D**, if the network topology has changed such that it can no longer use its route to **D** because a link along the route no longer works. When Route Maintenance indicates a source route is broken, **S** can attempt to use any other route it happens to know to **D**, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when **S** is actually sending packets to **D**.

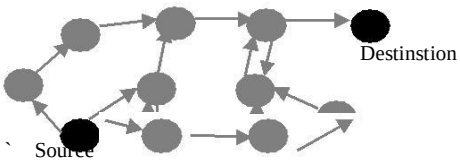

Fig.2: Route request (RREQ) broadcast flood

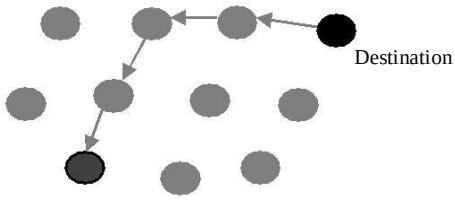

Fig.3:Route reply (RREP) propagation

III. EXPERIMENTAL RESULTS

A. Simulation Tables

The topology area has considered as 1000 mts * 1000 mts with a set of nodes placed randomly. Here, each node is initially placed at a position within the defined area. The simulation settings and parameters are described Table i. discrete event simulator NS 2.34 is used to simulate algorithm. In simulation, 20 mobile nodes move in a 1000 meter x 1000 meter square region for 10 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR).

i) Simulation Parameters

PARAMETERS	VALUES
Topology area	1000m×1000m
Simulation time	10 seconds
Radio propagation models	Two Ray Ground
Mobility model	Random way point
Interface queue	Drop tail queue
Number of nodes	20
Transmission power	0.987
Receiver power	0.812
Initial energy	30
Protocol	AODV
MAC protocol	802.11

B. Results

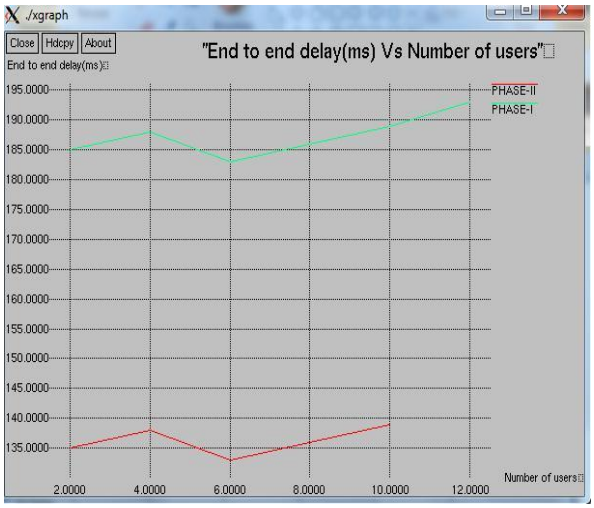

Fig.4:End to end delay

Fig.5: Communication Overhead

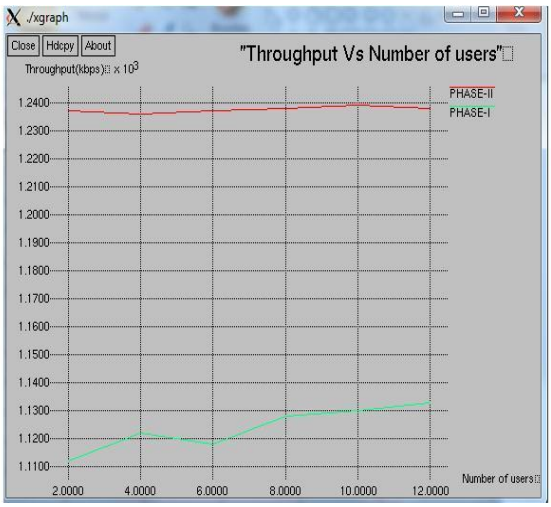

Fig.6: Throughput

In the last set of experimental, studied the communication overhead and end to end delay for delivering real packet to sink. In compare to the traffic normalization analysis reduces the communication overhead more than 92% and end to end delay is 60 %. Average End-to-End delay is a metrics used to measure performance with time taken by a pack to travel across a network from a source node to the destination node.Fig.4 as the number of communication users increase from 0 to 20 the value of delay can be increases the average deviation. Fig.5 Clustering technique which are to be used to reduce the communication overhead and increases network lifetime.Fig.6 As a number of node increases from 0 to 20 the value of average throughput also increases.

C. Equations

For convenience, we will reorganize the routing's main parameters into three elements:

1. $P = [P_{ij}]$ is an N × M matrix containing the router's forwarding policy. The value P_{ij} is the probability of sending to n_j a packet destined to d_i . Obviously, $0 \leq P_{ij} \leq 1$ and P_k j=1 $P_{ij} = 1$.
2. $C = [C_{ij}]$ is an N × M matrix representing the costs associated with each policy decision. Thus, $C_{ij} \geq 0$ measures the cost of using n_j as next hop for a packet destined to d_i . Unreachable nodes will be associated with an infinite cost, which in our model can be implemented by a sufficiently high cost value. These values are provided by the route discovery and maintenance mechanisms within the routing protocol.
3. D = [α_i] is the probability distribution of packets destined to di arriving at the router. The router can easily (re-)compute them periodically by using a sliding window over the amount of traffic received.

Despite its simplicity, this model is quite flexible and allow us to represent a broad range of different routing policies. For example, a minimum cost (e.g., shortest path) policy can be implemented as

$$P_{MC} = [P_{ij}] = \begin{cases} 1 & if\ C_{ij} \leq C_{ik}\ for\ k \neq j \\ 0 & otherwise \end{cases} \quad 1$$

Similarly, a random walk strategy is given by

$$P_{RR} = [P_{ij}] = \frac{1}{M}\ for\ all\ i,j \quad 2$$

All the information about a router's observable behavior in terms of link usage is implicitly encoded in P.

IV. CONCLUSION

Prior approaches on location privacy in sensor networks are mostly indented against local attackers and thus, can be easily failed by highly motivated global attackers. The present energy efficient network partition method against Global Attackers that effectively and efficiently maintains source location privacy. The presented EDSR-SRP method for collectively processing the packet interception times and eavesdropper locations at a fusion center. In this work, reduces the communication overhead and end to end delay for reporting event.

REFERENCES

[1] A.Proano, L.Lazos, M.Krunz. (2016),'Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs,'IEEE transaction on Mobile Computing.

[2] B.Alomair, A.Clark, J.Cuellar, and R.Poovendran. (2013), 'Toward a statistical framework for source anonymity in sensor networks,' IEEE Transactions on Mobile Computing, 12(2):248–260

[3] C.Ozturk, Y.Zhang, and Trappe. (2004), 'Source location privacy in energy-constrained sensor network routing, 'In proof the ACMSASN Workshop.

[4] G.Chinnu,N.Dhinakaran.(2012),'Protecting location privacy in wireless sensor networks against a local eavesdropper–a survey,' International Journal of Computer Applications, 56(5):25–47.

[5] J.A.Stankovic,A.D.WoodandT.He.(2011),'Realistic applications for wireless sensor networks.In theoretical aspects of Distributed computing in sensor network,'835-863.

[6] K.Bicakci, H.Gultekin, B, Tavli, and I.Bagci. (2011),'Maximizing lifetime of event-unobservable wireless sensor networks,' Computer Standards & Interfaces, 33(4):401–410.

[7] K.Mehta, D.Liu, M. Wright. (2012),' Protecting location privacy in sensor networks against a global eavesdropper,' IEEE Transactions on Mobile Computing, 11(2):320–336.

[8] K.Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie. (2000),' Protocols for self-organization of a wireless sensor network,' IEEE Personal Communications, 7(5):16–27.

[9] L.Lightfoot, Y.Li, J. Ren. (2010),' Preserving source-location privacy in wireless sensor network using STaR routing,' In Proc. of the IEEE GLOBECOM conference.